Introduction

The Labour Party is pleased that the Data Protection Act has committed the Information Commissioner to the production of an Age Appropriate Design Code. During the passage of the Bill, we expressed our support for Baroness Beeban Kidron's amendment to establish the Code and are pleased to contribute to this call for evidence on its design, the content of which will be critical to its success.

While the benefits of the digital economy are plentiful for Britain, it is clear that technology companies have fallen short in the design of their products and services in regard to respecting the rights of users over their data, particularly children, who make up around a third of online users.

In our response to the Internet Safety Strategy, the Labour Party expressed our concerns over the power imbalance between consumers and companies, specifically that "the online risks to children and young people rise every day as do the mental health concerns related to their use of the internet... the need for statutory protections is strong".

We expressed our disquiet, which remains, regarding the decision to stop the focus on children of the UK CCIS.

We stand by our position expressed in the ISS response that we must:

- not rely on industry self-regulation and
- ensure children and young people can benefit from the social and educational opportunities afforded by the Internet.

A well-crafted Code can protect children, not least in the area of privacy, while enabling innovation in the digital sector.

The Data Protection Act makes 18 the age below which the Code is relevant, in line with the UNCRC. This will be a challenge to the ISS which errs towards the ages of 13 or 16 as the points at which children are treated as adults in their use of the online platforms and products. The provision of the charter could usefully give the commissioner an overall tool by which to judge the standards of online services in each aspect of the code.

Below we have set out our answers to the specific questions. However, over and above this we propose:

1. A new Duty of Care, which should be created to bind the delivery of social media firms' services to children. This concept developed by the Carnegie Trust UK has several components. It would require firms to identify the harm or risk of harm to their users, and then take appropriate steps to both measure, report on and counter that harm. If the steps taken to diminish harm are not demonstrably effective, the Regulator needs step in rights to insist on change, or issue penalty notices. As Carnegie Trust argues, this draws on a tried and tested foundation of law stretching back to the 1974 Health and Safety at Work Act. These harms should include:
    - Harmful threats
    - Economic harm
    - Emotional harm
    - Harm to young people
    - Harms to justice and democracy

2. A class action regime to properly enable class actions in the courts to be brought against big firms on behalf of children. As we argued at Committee Stage of the Data Protection Bill, we believe we need a regime that allows citizens to bring actions in court. Article 81 of the GDPR basically allows group or class actions to be taken, but the Government proposes to activate that power by requiring an organisation bringing the class action to seek a positive authorisation from people affected. The risk is that that will create a burden so large that many organisations will simply not step up to the task. The alternative therefore is to change this, so that class actions can be brought by third party organisations with rights for consumers to opt out of the action.
3. A penalty regime that hits firms where it hurts – in their profits. We understand that the penalty regime for breach of this code is the same regime legislated in the Data Protection Bill. That implies that fines up to £18 million or 4% of global turnover. Crimes against children (specifically, "deliberate targeting of vulnerable victims") however are treated in Sentencing Guidelines as an aggravating factor in judging a crime, indicating higher culpability. We believe there is therefore grounds for consulting on a tougher regime of sanctions for breach of this code, with fines potentially levied on profits or cash on hand. For example, Google has cash on hand of over £90 billion. Sanctions need to be tough enough to incentive good behaviour from some of the biggest firms on earth. We believe that the proceeds of the fines should be paid into research and delivery of mental health services for children, especially those whose good mental health has been jeopardised by social media products.
4. Consideration must be given to requiring firms to make available to parents passwords for their children in the event of crimes against those children. For example, if a child is assaulted and evidence about perpetrators lies on a social media account, it is obviously an obstruction of justice for social media firms to deny access to those accounts to investigating authorities.
5. Finally, we remain of the view that a more powerful regulator is needed to police this landscape, and so we call on the Government to consider the proposals made by dot.evetyone for a single, powerful regulator with the scale and scope to police what the ICO has called a 'Wild West' effectively.

Outline responses to the ICO questions

1) The proposed age ranges are 3-5, 6-9, 10-12, 13-15 and 16-17. In terms of setting design standards for the processing of children's personal data by providers of ISS (online services), how appropriate you consider the above age brackets would be?
The age ranges for designing a Code as set out have our support if it is clear that the growing agency of the child is reflected in the Code. Their growing independence and their vulnerability have to be addressed. The Code cannot rely upon parents as a proxy for handling the behaviours of corporations.

2) Please provide any views or evidence about children's development needs in an online context for each, or any of the above age brackets.
We would suggest that due account is taken of the opinions of experts in this field such as Professor Sonia Livingstone and Professor Sarah Jayne Blakemore.

3) The Act requires the Commissioner to take into account the UK's obligations under the UN Convention on the Rights of the Child when drafting the Code. Please provide any views or evidence you have on how the Convention might apply in the context of setting design standards for the processing of children's personal data by providers of ISS (online services).

Articles 8 (identity), 12 (to be listened to), 13 (to share information), 14 (to meet friends/ join groups), 16 (to privacy), 17 (sourcing information), 29 (to education which builds respect, 36 (protection from harm to development) are all relevant but require clarity in the Code in terms of their application in the online environment.

4) The Government has provided the Commissioner with a list of areas which it proposes she should take into account when drafting the Code. Please provide any views or evidence you have on what you think the Information Commissioner should take into account when explaining the meaning and coverage of these terms in the Code.

   a) default privacy settings:

      i) There is no doubt that typically defaults are too low, inconsistent and fluid across platforms. This must change.

      ii) A high privacy setting should be required on all devices and for all online services likely to be accessed by a child.

      iii) The manner in which privacy is explained and settings expressed should be consistent across platforms so that children can readily understand them and do not become confused or bored. They must enable a child to make an informed decision.

      iv) Settings must always revert to high on closure.

      v) Any online interventions to entice or enable a child to avoid the repetitious consideration of their privacy should be challenged by the ICO.

   b) data minimisation standards:

      i) The communication by all ISS bodies must use age appropriate language. While the language standard may be age 13 for those who are younger it may mean a visual communication rather than words per se regarding terms and conditions or other commercial policies and commitments.

      ii) There should be no use of terms which when read literally by a child will mean one thing but in practice mean something much broader e.g. 'communicate with you'.

      iii) Privacy policies are those applied to adults if the site or device is linked to an adult e.g. a parent, even if the child is likely to use it. This is not appropriate. If the likely user is the child the privacy policy the parent sees for their 5 year old should be a child age appropriate policy.

      iv) When a holder of an account used by a child closes the account all data held should be deleted automatically. There should be no enticements to the child to give permission to the ISS retaining the data. The child should be sent a copy of the data before deletion if they so request.

   c) the presentation and language of terms and conditions and privacy notices:

      i) Terms and conditions should be communicated at an age appropriate level within 75 seconds rising to 90 seconds dependent on age. Links to more detail may be included.

      ii) The use of visual tools is welcome

iii) The length and complexity must be in line with the language developmental stage of each age group of children.

iv) T & C language must not rise above the typical reading age of a 13 year old even when the target market is 15-17 year olds. A maximum word count would be preferable.

v) Where it is proven (and a standard of proof should be set) that children cannot understand the T & C then the ICO will find a breach of the Code and take action.

vi) Online services must uphold their own published T & C. Routine failure to do so should be considered a breech of the code. That way children and parents can have confidence in what services say they are going to do, including regarding the age of the child.

d) uses of geolocation technology:

i) Geolocation must be off by default and switch off after each use. While there may be cases of safety and risk to be managed a default position cannot be to track children. Even when there is a case for tracking a child should know and should be able to see when the tracking is activated.

ii) If a child gives their permission to be tracked. They must be able to withdraw that permission. It should not be conditional. Nor should tracking be transferred from a purpose for which it was agreed or requested by a child to another purpose to which they have no knowledge or understanding.

iii) At no point can a commercial body use the data from tracking to inform sales or other purposes. This is of paramount importance as it can reinforce disadvantages already facing children due to the area in which they live.

e) automated and semi-automated profiling:

i) Automated profiling can include geolocation or home postcodes. This should not be allowed for children as it risks prejudicing their access to services and the way in which their potential is interpreted.

ii) A child must be able to understand how and why they are being profiled including by education and health services

iii) Profiling must have a specific life expectancy and not be held across a lifespan. The ICO standards should be clear about an expiry date.

f) transparency of paid-for activity such as product placement and marketing:

i) Where content is placed on a site which children are likely to use to promote a product or service to them and for which the site gains income the fact of that earning should be made explicit.

ii) Any data which can be drawn through the activity of a child on the site as well as their personal data must not be processed to inform advertising. This would amount to commercial exploitation of a child which is unacceptable.

iii) Education on the commercial intent through promotions, presentation, product placement, special offers on line should be included in PSHE and other relevant curriculum topics.

g) the sharing and resale of data:

   i) This should be limited when the data belongs to under 18's. It should provide a financial benefit to them, even if very small and be agreed each time the data would be shared and resold. There are existing models for such payments in such as the music industry.

   ii) Where the child is too young to hold an account to receive the funding this must be held in trust for them by parents or a trusted adult for access at an agreed age.

   iii) The ASA guidance on enhanced disclosures should be included and adjusted to reflect the developmental stages defined in the Code.

h) the strategies used to encourage extended user engagement:

   i) The Code should clearly define the 'persuasive design characteristics'.

   ii) The Code should expect the ISS using persuasive design strategies to have checked and confirmed the age of its child users. To not have done so would be a breach of the Code.

i) user reporting and resolution processes and systems:

   i) The Code should include universal reporting standards

   ii) The child who challenges the use of their data to the ICO must have a right of redress, a right to be heard and a right of appeal on any decision made.

   iii) No child should be charged for activating their data rights

j) the ability to understand and activate a child's right to erasure, rectification and restriction:

   i) As a child develops their views on what they may have inadvertently shared at an earlier age will modify. Throughout childhood there will be risks to sharing data which a child understood to be private or temporary. Therefore the child must have the right to remove their data throughout their childhood and again when they are adults reflecting on their past. This can be delivered most efficiently by the removal of all data automatically by social media accounts unless the child actively requests that it remains as might be the case with such as study project content or family content. There is a case for data expiry especially in relation to social media words and images as well as game records and inappropriate use of language, accessing inappropriate sites such as gambling and pornography.

k) the ability to access advice from independent, specialist advocates on all data rights:

   i) This should be freely available to a child on conditions set out in the Code.

l) any other aspect of design that the commissioner considers relevant:

   i) A kitemark or certification system should be established to show users whether the standards have been met.

5) Please provide any views or evidence you have on the following:

   a) The opportunities and challenges you think might arise in setting design standards for the processing of children's data by providers of ISS (online services)

i) By adopting the Code the ISS industry will build itself up as an ethical trade which is currently not the public view of it. Complexities and costs of adopting the Code must be solved by industry and not used as avoidance tactics. There will be costs to the providers of ISS but as these companies invest in their own strategic development and increase their investments in new lines of activity this should not be regarded as an additional cost.

ii) For smaller businesses the key will be simplicity of the Code.

iii) There is scope for business innovation and the expansion of opportunities for web developers, technical support services and personal data management and privacy services.

b) How the ICO working with relevant stakeholders might use the opportunities presented and positively address any challenges you have identified

i) The asymmetry of power between children and industry has to be addressed given the rise in stress among children, including damage to self-esteem through to mental ill-health.

c) What design standards might be appropriate in any of the above areas and for any of the proposed age brackets

i) The bars cannot be set on an assumption that parents have a controlling role when a child reaches the age of 13. The bars should commence with parental delegation of the child's rights when they are 3-5 and over time move to complete independence. This will include a period of dual oversight with the decisions being made by the child with oversight from the parent. Parents have a responsibility to educate themselves about the workings of the Code. Parents cannot be left with the responsibility to handle corporate behaviours.

d) Examples of ISS design you consider to be good practice

e) About any additional areas, not included in the list above that you think should be the subject of a design standard

i) Childhood Data Impact Assessments as standard for all existing services and products, and new services and products prior to launch. Building on the GDPR's requirement for Data Protection Impact Assessments for all processing that is likely to have a high risk to the rights and freedoms of users and the ICO's guidance on the circumstances where DIPA is required, we support 5Rights' recommendation for Child Data Impact Assessments (CDIA) for all online services likely to be accessed by a child. The CDIA would address the specific needs and higher standards to which children are entitled, and place the requirement to carry out such assessments on a statutory footing. Introducing Child Data Impact Assessments before services and products are rolled out would circumvent some of the most obvious data risks.